

11 Curve Ellittiche

11.1 Curve Algebriche

Sia \mathbb{K} un campo, $(\mathbb{K}^3)^* = \mathbb{K}^3 \setminus \{(0,0,0)\}$ e si consideri lo spazio vettoriale $(\mathbb{K}^3, +, \cdot)$. Siano $(x_1, x_2, x_3), (x'_1, x'_2, x'_3)$ due elementi di $(\mathbb{K}^3)^*$, definiamo la seguente relazione binaria:

$$(x_1, x_2, x_3) \sim (x'_1, x'_2, x'_3) \iff \exists \lambda \in \mathbb{K} \setminus \{0\} \text{ tale che } (x_1, x_2, x_3) = \lambda (x'_1, x'_2, x'_3).$$

Chiaramente \sim è una relazione di equivalenza su $(\mathbb{K}^3)^*$ e l'insieme quoziente $(\mathbb{K}^3)^* / \sim$, che si denota con $PG(2, \mathbb{K})$, si dice **piano proiettivo sul campo \mathbb{K}** .

Il generico elemento di $PG(2, \mathbb{K})$, detto **punto**, è:

$$[(x_1, x_2, x_3)]_{\sim} = \{\lambda (x_1, x_2, x_3) \text{ t.c. } \lambda \in \mathbb{K} \setminus \{0\}\}.$$

Chiaramente i punti di $PG(2, \mathbb{K})$ sono i sottospazi 1-dimensionali di \mathbb{K}^3 privati del vettore nullo. Per semplicità, un punto P di $PG(2, \mathbb{K})$ verrà indicato con un suo rappresentante, cioè se P è individuato da $[(x_1, x_2, x_3)]_{\sim}$ allora scriveremo $P = (x_1, x_2, x_3)$ tenendo presente che la terna (x_1, x_2, x_3) è data a meno di un fattore di proporzionalità non nullo. La terna (x_1, x_2, x_3) rappresenta le **coordinate proiettive omogenee** di P .

Definiamo **rette** di $PG(2, \mathbb{K})$ i sottospazi 2-dimensionali (piani vettoriali) di \mathbb{K}^3 privati del vettore nullo. Ogni piano vettoriale ha chiaramente equazione $ax_1 + bx_2 + cx_3 = 0$ dove $(a, b, c) \in (\mathbb{K}^3)^*$ sono individuati a meno di un fattore di proporzionalità non nullo. Pertanto, possiamo rappresentare la generica retta di $PG(2, \mathbb{K})$ con la scrittura $[a, b, c]$ a meno di un fattore di proporzionalità non nullo. La terna $[a, b, c]$ rappresenta le **coordinate proiettive omogenee** della generica retta di $PG(2, \mathbb{K})$.

I punti di $PG(2, \mathbb{K})$ che giacciono sulla **retta impropria** $r_{\infty}: x_3 = 0$ sono detti **punti impropri**. I punti di $PG(2, \mathbb{K})$ che hanno $x_3 \neq 0$ sono detti **punti propri**.

L'insieme $AG(2, \mathbb{K}) = PG(2, \mathbb{K}) \setminus r_{\infty}$, è detto **piano affine**. Il generico punto proprio $Q = (x_1, x_2, x_3)$ ($x_3 \neq 0$) corrisponde al punto di $AG(2, \mathbb{K})$ di coordinate $(x, y) = \left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right)$.

Definizione 11.1. (Curva Algebrica Piana di ordine n)

Si dice **curva algebrica piana di ordine n** , l'insieme dei punti di $PG(2, \mathbb{K})$ le cui coordinate proiettive verificano un'equazione del tipo $F(x_1, x_2, x_3) = 0$ dove $F(x_1, x_2, x_3)$ è un polinomio omogeneo di grado n a coefficienti in \mathbb{K} , nelle variabili x_1, x_2, x_3 . In generale una curva algebrica di ordine n si indica con \mathcal{C}^n e $F(x_1, x_2, x_3) = 0$ si dice **equazione di \mathcal{C}^n in coordinate proiettive omogenee**.

Ricordiamo che un polinomio $F(x_1, x_2, x_3)$ di grado n è omogeneo se e solo se $F(\lambda x_1, \lambda x_2, \lambda x_3) = \lambda^n F(x_1, x_2, x_3)$ per ogni $\lambda \in \mathbb{K}, \lambda \neq 0$.

Le curve algebriche $\mathcal{C}^1, \mathcal{C}^2, \mathcal{C}^3$ sono le rette, le coniche, le cubiche, rispettivamente:

$$\begin{aligned}\mathcal{C}^1 & : a_1x_1 + a_2x_2 + a_3x_3 = 0; \\ \mathcal{C}^2 & : a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_1x_2 + a_5x_1x_3 + a_6x_2x_3 = 0; \\ \mathcal{C}^3 & : a_1x_1^3 + a_2x_2^3 + a_3x_3^3 + a_4x_1x_2x_3 + a_5x_1^2x_2 + a_6x_1x_2^2 + \\ & \quad a_7x_1^2x_3 + a_8x_1x_3^2 + a_9x_2^2x_3 + a_{10}x_2x_3^2 = 0.\end{aligned}$$

In seguito, limiteremo la nostra attenzione alle sole cubiche.

Definizione 11.2. (Punto semplice e doppio)

Un punto P_0 di una cubica \mathcal{C}^3 si dice **punto semplice** se ogni retta per P_0 , eccetto una retta, ha una sola intersezione con \mathcal{C}^3 in P_0 . La retta che fa eccezione ha più di una intersezione con \mathcal{C}^3 in P_0 e si chiama **tangente principale**.

P_0 si dice **punto doppio** di \mathcal{C}^3 se ogni retta per P_0 , eccetto due rette, ha due intersezioni con \mathcal{C}^3 in P_0 . Le rette che fanno eccezione hanno più di due intersezioni con \mathcal{C}^3 in P_0 e si chiamano **tangenti principali** in P_0 a \mathcal{C}^3 .

Proposizione 11.3. Sia \mathcal{C}^3 una cubica di equazione $F(x_1, x_2, x_3) = 0$ e sia $P_0 = (x_1^0, x_2^0, x_3^0)$ un suo punto. Indicate con F_i ed F_{ij} ($i, j = 1, 2, 3$) le derivate parziali formali prime e seconde di $F(x_1, x_2, x_3)$ rispettivamente, allora

$$\begin{aligned}P_0 \text{ è semplice} & \Leftrightarrow (F_1^0, F_2^0, F_3^0) \neq (0, 0, 0) \text{ e l'equazione della} \\ & \text{tangente principale in } P_0 \text{ è } F_1^0x_1 + F_2^0x_2 + F_3^0x_3 = 0; \\ P_0 \text{ è doppio} & \Leftrightarrow F_1^0 = F_2^0 = F_3^0 = 0 \text{ e almeno una tra le} \\ & F_{ij}^0 \neq 0. \text{ In tal caso, l'equazione complessiva} \\ & \text{delle tangenti principali è una conica degenera} \\ & \text{di equazione } \sum_{i,j=1}^3 F_{ij}^0 x_i x_j = 0.\end{aligned}$$

Siano \mathcal{C}^3 una cubica su un campo \mathbb{K} e P_0 un suo punto.

- Se P_0 è un punto doppio, allora l'equazione complessiva delle tangenti principali a \mathcal{C}^3 in P_0 consiste dell'unione di due rette ℓ_1 ed ℓ_2 . Risulta che il punto P_0 si dice **cuspidale** se ℓ_1 ed ℓ_2 sono coincidenti, **nodo** se ℓ_1 ed ℓ_2 sono distinte ed hanno coefficienti in \mathbb{K} , **punto doppio isolato** se ℓ_1 ed ℓ_2 sono distinte ed hanno coefficienti in un'estensione quadratica di \mathbb{K} .
- Se P_0 è un punto semplice, allora esso si dice **ordinario** se la tangente in P_0 ha esattamente due intersezioni con \mathcal{C}^3 in P_0 e **flesso di prima specie** se la tangente ha esattamente tre intersezioni con \mathcal{C}^3 in P_0 .

Definizione 11.4. Una cubica \mathcal{C}^3 di equazione in coordinate omogenee $F(x_1, x_2, x_3) = 0$ si dice **riducibile** se il polinomio si scrive nella forma

$$F(x_1, x_2, x_3) = G_1(x_1, x_2, x_3) \cdot G_2(x_1, x_2, x_3)$$

con $G_1(x_1, x_2, x_3)$ e $G_2(x_1, x_2, x_3)$ polinomi di grado 1 e 2, rispettivamente.

Se poniamo $\mathcal{C}_1 : G_1(x_1, x_2, x_3) = 0$ e $\mathcal{C}_2 : G_2(x_1, x_2, x_3) = 0$, diremo che la curva è l'unione delle sue componenti \mathcal{C}_1 e \mathcal{C}_2 .

Osservazione 11.5. Sia $F(x_1, x_2, x_3) = 0$ l'equazione in coordinate omogenee di una cubica \mathcal{C}^3 . Allora

$$\mathcal{C}^3 \cap AG(2, \mathbb{K}) = \{(x_1, x_2, x_3) \in \mathcal{C}^3 : x_3 \neq 0\}.$$

Pertanto, per tali punti, vale che

$$\begin{aligned} F(x_1, x_2, x_3) &= \sum_{0 \leq p+q \leq 3} a_{pq} x_1^p x_2^q x_3^{3-(p+q)} = \\ &= \sum_{0 \leq p+q \leq 3} a_{pq} x_3^3 \left(x_1^p x_2^q x_3^{-(p+q)} \right) = \\ &= x_3^3 \sum_{0 \leq p+q \leq 3} a_{pq} \left(\frac{x_1}{x_3} \right)^p \left(\frac{x_2}{x_3} \right)^q = \\ &= x_3^3 f\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right) = \\ &= x_3^3 f(x, y). \end{aligned}$$

Quindi $f(x, y) = 0$ si dice **equazione affine della cubica \mathcal{C}^3** .

Ora esprimiamo analiticamente i concetti di punto semplice o punto doppio nel caso affine.

Proposizione 11.6. Sia \mathcal{C}^3 una cubica di equazione $f(x, y) = 0$ in coordinate affini e sia $P_0 = (x_0, y_0)$ un suo punto. Allora

$$\begin{aligned}
 P_0 \text{ è semplice} &\Leftrightarrow (f_x^0, f_y^0) \neq (0, 0) \text{ e l'equazione della} \\
 &\text{tangente principale in } P_0 \text{ è} \\
 &f_x^0(x - x_0) + f_y^0(y - y_0) = 0; \\
 P_0 \text{ è doppio} &\Leftrightarrow f_x^0 = f_y^0 = 0 \text{ e almeno una tra le derivate} \\
 &\text{parziali seconde di } f \text{ calcolate in } (x_0, y_0) \text{ è} \\
 &\text{diversa da 0. In tal caso, l'equazione} \\
 &\text{complessiva delle tangenti principali è} \\
 &f_{xx}^0(x - x_0)^2 + 2f_{xy}^0(x - x_0)(y - y_0) + \\
 &+ f_{yy}^0(y - y_0)^2 = 0.
 \end{aligned}$$

Definizione 11.7. Una cubica \mathcal{C}^3 si dice **non singolare** se e solo se tutti i suoi punti sono semplici.

Definizione 11.8. Una cubica \mathcal{C}^3 di equazione $f(x, y) = 0$ in coordinate affini si dice **riducibile** se

$$f(x, y) = g_1(x, y) \cdot g_2(x, y)$$

con $g_1(x, y)$ e $g_2(x, y)$ polinomi di grado 1 e 2, rispettivamente.

Teorema 11.9. Una cubica irriducibile \mathcal{C}^3 ha al più un punto doppio.

Dimostrazione. Supponiamo per assurdo che \mathcal{C}^3 abbia almeno due punti doppi, cioè supponiamo che $P_1, P_2 \in \mathcal{C}^3$, $P_1 \neq P_2$ siano dei punti doppi. Indicata con P_1P_2 la retta passante per P_1 e P_2 , si ha che

$$|P_1P_2 \cap \mathcal{C}^3| \geq 2 + 2 = 4,$$

pertanto P_1P_2 è una componente di \mathcal{C}^3 per il **Teorema di Bezout**, ma ciò contraddice l'irriducibilità di quest'ultima.

□

Quindi una cubica è

1. riducibile se si può esprimere come unione di tre rette o come unione di una retta e di una conica non degenera;
2. singolare se e solo se contiene un punto doppio.

Nel 1935, **Trygve Nagell**, pubblicò un procedimento per trasformare una cubica irriducibile, non singolare, avente un punto \mathbb{K} -razionale, nella **forma di Weierstrass**:

$$y^2 + y(a_1x + a_3) = x^3 + a_2x^2 + a_4x + a_6.$$



Figura 11.1: Trygve Nagell (1895-1988)

Teorema 11.10. *Sia \mathcal{C}^3 una cubica, nel piano affine $AG(2, \mathbb{K})$ si può effettuare un cambiamento di coordinate in modo tale che nel nuovo sistema di coordinate si verifichi:*

a) *se $\text{char}(\mathbb{K}) \neq 2, 3$, la curva \mathcal{C}^3 ha equazione*

$$y^2 = x^3 + Ax + B; \quad (11.1)$$

b) *se $\text{char}(\mathbb{K}) = 3$, la curva \mathcal{C}^3 ha equazione*

$$y^2 = x^3 + Ax^2 + Bx + C; \quad (11.2)$$

c) (i) *se $\text{char}(\mathbb{K}) = 2$ e $a_1 = 0$, l'equazione è del tipo:*

$$y^2 + Cy = x^3 + Ax + B \quad (11.3)$$

*ed in tal caso \mathcal{C}^3 si dice **supersingolare**;*

(ii) *se $\text{char}(\mathbb{K}) = 2$ e $a_1 \neq 0$, l'equazione è del tipo:*

$$y^2 + xy = x^3 + Ax^2 + B \quad (11.4)$$

*ed in tal caso \mathcal{C}^3 si dice **non supersingolare**.*

*Le equazioni del tipo (11.1) – (11.4) si dicono **equazioni di Weierstrass** di una cubica.*

Dimostrazione. Per il risultato di **Nagell**, una cubica (non singolare, irriducibile e con un punto \mathbb{K} -razionale) si può sempre scrivere nella forma

$$y^2 + y(a_1x + a_3) = x^3 + a_2x^2 + a_4x + a_6. \quad (11.5)$$

Supponiamo che $\text{char}(\mathbb{K}) \neq 2$. Allora, nell'equazione (11.5) si può effettuare il seguente cambiamento di coordinate:

$$\begin{cases} x &= X \\ y &= Y - \frac{a_1X + a_3}{2} \end{cases}$$

ottenendo:

$$\left(Y - \frac{a_1X + a_3}{2}\right)^2 + \left(Y - \frac{a_1X + a_3}{2}\right)(a_1X + a_3) = X^3 + a_2X^2 + a_4X + a_6.$$

Da tale equazione segue che

$$Y^2 - \frac{a_1^2X^2}{4} - \frac{a_3^2}{4} - \frac{a_1a_3X}{2} = X^3 + a_2X^2 + a_4X + a_6$$

e quindi l'equazione (11.5) nelle nuove coordinate è:

$$Y^2 = X^3 + \left(a_2 + \frac{a_1^2}{4}\right)X^2 + \left(a_4 + \frac{a_1a_3}{2}\right)X + \left(a_6 + \frac{a_3^2}{4}\right)$$

cioè essa è della forma:

$$Y^2 = X^3 + AX^2 + BX + C \quad (11.6)$$

con $A = \left(a_2 + \frac{a_1^2}{4}\right)$, $B = \left(a_4 + \frac{a_1a_3}{2}\right)$ e $C = \left(a_6 + \frac{a_3^2}{4}\right)$. Questo prova l'asserto (b).

Inoltre, se la caratteristica del campo \mathbb{K} è diversa anche da 3, si può considerare nell'equazione (11.6) un ulteriore cambiamento di coordinate effettuando la seguente sostituzione:

$$\begin{cases} X &= \tilde{X} - \frac{A}{3} \\ Y &= \tilde{Y} \end{cases}$$

Otteniamo così:

$$\tilde{Y}^2 = \left(\tilde{X} - \frac{A}{3}\right)^3 + A\left(\tilde{X} - \frac{A}{3}\right)^2 + B\left(\tilde{X} - \frac{A}{3}\right) + C$$

da cui ricaviamo

$$\tilde{Y}^2 = \tilde{X}^3 + \left(B - \frac{A^2}{3}\right)\tilde{X} + \left(\frac{2}{27}A^3 - \frac{AB}{3} + C\right).$$

Pertanto, l'equazione (11.6) nelle nuove coordinate, sarà della forma

$$\tilde{Y}^2 = \tilde{X}^3 + A'\tilde{X} + B'$$

con $A' = \left(B - \frac{A^2}{3}\right)$ e $B' = \left(\frac{2}{27}A^3 - \frac{AB}{3} + C\right)$, che è l'asserto (a).

Infine supponiamo che $\text{char}\mathbb{K} = 2$, consideriamo l'equazione (11.5) e distinguiamo due casi.

Se $a_1 = 0$, effettuiamo il seguente cambiamento di coordinate:

$$\begin{cases} x &= X + a_2 \\ y &= Y \end{cases}$$

ottenendo così:

$$Y^2 + a_3Y = (X + a_2)^3 + a_2(X + a_2)^2 + a_4(X + a_2) + a_6$$

da cui segue:

$$Y^2 + a_3Y = X^3 + 3X^2a_2 + 3Xa_2^2 + a_2^3 + a_2X^2 + 2a_2^2X + a_2^3 + a_4X + a_2a_4 + a_6.$$

Ricordando che $\text{char}\mathbb{K} = 2$, otteniamo:

$$Y^2 + a_3Y = X^3 + (a_2^2 + a_4)X + (a_2a_4 + a_6).$$

Tale equazione è della forma

$$Y^2 + CY = X^3 + AX + B.$$

con $C = a_3$, $A = a_2^2 + a_4$, $B = a_2a_4 + a_6$. Pertanto, nel caso $a_1 = 0$, si ha un'equazione del tipo (11.3).

Se $a_1 \neq 0$, consideriamo nell'equazione (11.5) la seguente trasformazione

$$\begin{cases} x &= a_1^2X + a_1^{-1}a_3 \\ y &= a_1^3Y + a_1^{-3}(a_1^2a_4 + a_3^2) \end{cases}$$

Risulta:

$$(a_1^3Y + a_1^{-1}a_4 + a_1^{-3}a_3^2)^2 + (a_1^3Y + a_1^{-1}a_4 + a_1^{-3}a_3^2)(a_1(a_1^2X + a_1^{-1}a_3) + a_3)$$

che a sua volta è uguale a

$$(a_1^2X + a_1^{-1}a_3)^3 + a_2(a_1^2X + a_1^{-1}a_3)^2 + a_4(a_1^2X + a_1^{-1}a_3) + a_6,$$

da cui segue

$$\begin{aligned} a_1^6Y^2 + a_1^6XY &= a_1^6X^3 + (a_1^3a_3 + a_2a_1^4)X^2 + \\ &+ (a_1^{-3}a_3^3 + a_2a_1^{-2}a_3^2 + a_4a_1^{-1}a_3 - a_1^{-2}a_4^2 - a_1^{-6}a_3^4 + a_6). \end{aligned}$$

Poichè $a_1 \neq 0$ possiamo dividere per a_1^6 , ottenendo l'equazione

$$\begin{aligned} Y^2 + XY &= X^3 + (a_1^{-3}a_3 + a_2a_1^{-2})X^2 + \\ &+ (a_1^{-9}a_3^3 + a_2a_1^{-8}a_3^2 + a_4a_1^{-7}a_3 - a_1^{-8}a_4^2 - a_1^{-12}a_3^4 + a_6a_1^{-6}) \end{aligned}$$

che è del tipo:

$$Y^2 + XY = X^3 + AX^2 + B$$

con coefficienti: $B = (a_1^{-9}a_3^3 + a_2a_1^{-8}a_3^2 + a_4a_1^{-7}a_3 - a_1^{-8}a_4^2 - a_1^{-12}a_3^4 + a_6a_1^{-6})$ e $A = (a_1^{-3}a_3 + a_2a_1^{-2})$ cioè un'equazione del tipo (11.4).

□

Per il **Teorema 11.10**, in seguito considereremo sempre cubiche rappresentate da un'equazione di Weierstrass, tenendo presente che il loro punto improprio, che denoteremo con ∞ , ha coordinate proiettive omogenee $(0, 1, 0)$.

Poiché è facile vedere che il punto ∞ non è mai doppio per una cubica rappresentata da un'equazione di Weierstrass, dalla **Proposizione 11.6** segue che l'eventuale punto doppio di una cubica in forma di Weierstrass è proprio e quindi ha coordinate (x_0, y_0) tali che $f_x(x_0, y_0) = f_y(x_0, y_0) = 0$.

Definizione 11.11. (Curva Ellittica)

Una cubica non singolare di $AG(2, \mathbb{K})$ rappresentata, a seconda della caratteristica del campo, da una delle equazioni di Weierstrass (11.1) – (11.4) del **Teorema 11.10**, si dice **curva ellittica**.

Teorema 11.12. *Valgono i seguenti risultati:*

- 1) Se $\text{char}(\mathbb{K}) \neq 2, 3$, allora la cubica di equazione

$$y^2 = x^3 + Ax + B$$

è singolare se e solo se vale $27B^2 + 4A^3 = 0$;

- 2) Se $\text{char}(\mathbb{K}) = 3$, allora la cubica di equazione

$$y^2 = x^3 + Ax^2 + Bx + C$$

è singolare se e solo se vale $-A^3C + A^2B^2 - B^3 = 0$;

- 3) Se $\text{char}\mathbb{K} = 2$, si verifica che:

- (i) la cubica di equazione

$$y^2 + Cy = x^3 + Ax + B$$

è singolare se e solo se $C = 0$;

- (ii) la cubica di equazione

$$y^2 + xy = x^3 + Ax^2 + B$$

è singolare se e solo se $B = 0$.

Dimostrazione. Se $\text{char}(\mathbb{K}) \neq 2, 3$, C^3 ha equazione

$$y^2 = x^3 + Ax + B.$$

Affinchè C^3 sia singolare, si deve verificare che: $f_y = 2y = 0$ e $f_x = 3x^2 + A = 0$. Cioè la cubica è singolare se e solo se

$$x^3 + Ax + B = 0, \tag{11.7}$$

ed inoltre

$$x^2 = -\frac{A}{3}, \tag{11.8}$$

rispettivamente.

Sostituendo tale valore di x^2 in (11.7) si ha:

$$x\left(-\frac{A}{3}\right) + Ax + B = 0$$

da cui segue:

$$\frac{2}{3}Ax + B = 0. \quad (11.9)$$

Se $A \neq 0$, da (11.9) si ottiene $x = -\frac{3B}{2A}$. Sostituendo quest'ultima espressione in (11.8), otteniamo $\frac{9B^2}{4A^2} = -\frac{A}{3}$. Pertanto segue che, in questo caso, condizione necessaria e sufficiente affinché \mathcal{C}^3 sia singolare, è che:

$$27B^2 + 4A^3 = 0. \quad (11.10)$$

Se $A = 0$, allora condizione affinché \mathcal{C}^3 sia singolare, è che sia $B = 0$ e quindi anche in questo caso la condizione di singolarità della cubica può essere espressa ancora dalla (11.10).

Se $\text{char}(\mathbb{K}) = 3$, \mathcal{C}^3 ha equazione $y^2 = x^3 + Ax^2 + Bx + C$ e affinché \mathcal{C}^3 sia singolare, si deve verificare che $f_y = 2y = 0$ e $f_x = 3x^2 + 2Ax + B = 0$. Dalla prima condizione segue che

$$x^3 + Ax^2 + Bx + C = 0 \quad (11.11)$$

mentre la derivata rispetto ad x diventa $2Ax + B = 0$.

Se $A \neq 0$, si ha che $x = -\frac{B}{2A}$ e sostituendo tale valore di x in (11.11), si ottiene

$$-\frac{B^3}{8A^3} + \frac{AB^2}{4A^2} - \frac{B^2}{2A} + C = 0,$$

da cui segue $\frac{-B^3+2A^2B^2-4A^2B^2+8A^3C}{8A^3} = 0$. Pertanto, in questo caso, poichè $\text{char}\mathbb{K} = 3$, condizione necessaria e sufficiente affinché \mathcal{C}^3 sia singolare, è che:

$$-A^3C + A^2B^2 - B^3 = 0 \quad (11.12)$$

Se $A = 0$, allora condizione affinché \mathcal{C}^3 sia singolare, è che sia $B = 0$ e quindi anche in questo caso la condizione di singolarità della cubica può essere ancora espressa dalla (11.12).

Se $\text{char}\mathbb{K} = 2$, bisogna distinguere due sottocasi:

(i) \mathcal{C}^3 ha equazione $y^2 + Cy = x^3 + Ax + B$.

Analogamente ai casi precedenti, si deve verificare che:

$$f_y = 2y + C = 0 \text{ e } f_x = 3x^2 + A = 0.$$

Da tali equazioni, segue rispettivamente: $C = 0$ e $x^2 + A = 0$ che equivale a $x^2 = A$. Sostituendo tali risultati nell'equazione della \mathcal{C}^3 , si ottiene $y^2 = Ax + Ax + B$ da cui segue $y^2 = B$. Quindi il punto di coordinate $(x, y) = (\sqrt{A}, \sqrt{B})$ è un punto doppio (si noti che in un campo a caratteristica 2, tutti gli elementi sono quadrati).

(ii) \mathcal{C}^3 ha equazione $y^2 + xy = x^3 + Ax^2 + B$.

In tal caso si deve verificare che

$$f_y = 2y + x = 0 \text{ e } f_x = 3x^2 + 2Ax - y = 0.$$

Da tali condizioni segue che $x = 0$ e $y = 0$. Sostituendo i valori di x e y appena trovati nell'equazione di \mathcal{C}^3 si ottiene che, in questo caso, condizione necessaria e sufficiente affinché la cubica sia singolare, è che sia $B = 0$.

□

Osservazione 11.13. Osserviamo che il **Teorema 11.12** fornisce delle condizioni necessarie e sufficienti affinché una cubica in forma di Weierstrass sia una curva ellittica.

Abbiamo visto che una cubica è singolare se e solo se contiene un punto doppio. In tal caso, il seguente Teorema descrive l'equazione della cubica e le equazioni delle tangenti alla curva nel punto doppio, nel caso che questo sia una cuspidi, un nodo o un punto doppio isolato.

Teorema 11.14. *Supponiamo che $\text{char}\mathbb{K} \neq 2, 3$ e consideriamo una generica \mathcal{C}^3 su \mathbb{K} . Valgono i seguenti risultati:*

- (i) *Se \mathcal{C}^3 ha una cuspidi, essa ha coordinate $(0,0)$. Allora la cubica ha equazione $y^2 = x^3$ e l'equazione complessiva delle tangenti in $(0,0)$ è $y^2 = 0$.*
- (ii) *Se \mathcal{C}^3 ha un nodo o un punto doppio isolato allora, dopo un'opportuna trasformazione affine, esso ha coordinate $(0,0)$, la cubica ha equazione $y^2 = x^2(x+a)$ ($a \neq 0$) e le tangenti nel suo punto doppio hanno equazione $y - \alpha x = 0$ e $y + \alpha x = 0$, dove $\alpha^2 = a$ e $\alpha \in \mathbb{K}$ nel caso del nodo o $\alpha \notin \mathbb{K}$ nel caso del punto doppio isolato.*

Dimostrazione. Dalla dimostrazione del **Teorema 11.12** segue che l'eventuale punto doppio di una cubica di equazione $y^2 = x^3 + Ax + B$ ha come prima coordinata una radice multipla del trinomio $x^3 + Ax + B$. Quindi si possono verificare due possibilità: $x^3 + Ax + B$ ha una radice tripla o doppia.

- Supponiamo che $x^3 + Ax + B$ abbia una radice tripla x_0 . Allora x_0 è radice doppia e semplice delle derivate formali prime e seconde di $y^2 = x^3 + Ax + B$ rispettivamente. Poiché la derivata formale seconda è $6x$, allora $x_0 = 0$. Quindi $A = B = 0$ e pertanto la curva ha equazione

$$y^2 = x^3. \quad (11.13)$$

e il suo unico punto singolare ha coordinate $(0,0)$. Per la **Proposizione 11.6** l'equazione complessiva delle tangenti principali in $(0,0)$ ad \mathcal{E} , è data da $y^2 = 0$. Pertanto $(0,0)$ è una cuspide per (11.13).

- Supponiamo ora che $x^3 + Ax + B$ abbia una radice doppia x_0 . Allora x_0 è radice semplice della derivata formale prima $3x^2 + A$. Pertanto si ha che:

$$x_0^3 + Ax_0 + B = 0 \quad (11.14)$$

ed inoltre

$$3x_0^2 + A = 0, \quad (11.15)$$

rispettivamente. Da (11.15) segue che $x_0^2 = -\frac{A}{3}$. Sostituendo tale valore in (11.14) si ottiene $x_0(-\frac{A}{3}) + Ax_0 + B = 0$ da cui segue che, se $A \neq 0$, $x_0 = -\frac{3B}{2A}$. Pertanto, l'unico punto singolare della cubica ha coordinate $(x_0, y_0) = (-\frac{3B}{2A}, 0)$. Se consideriamo la trasformazione affine:

$$\begin{cases} X &= x + \frac{3B}{2A} \\ Y &= y, \end{cases} \quad (11.16)$$

possiamo assumere che anche in questo caso l'unico punto singolare della curva sia il punto di coordinate $(0,0)$. Per trovare l'equazione della cubica, osserviamo che, essendo x_0 una radice doppia di $x^3 + Ax + B$, possiamo scrivere

$$y^2 = \left(x + \frac{3B}{2A}\right)^2 (x - x_1)$$

dove x_1 è una radice semplice del trinomio che descrive la curva. Effettuando il cambiamento di coordinate (11.16), si ha che

$$Y^2 = \left(X - \frac{3B}{2A} + \frac{3B}{2A}\right)^2 \left(X - \frac{3B}{2A} - x_1\right) = X^2 (X + a)$$

dove $a = -\frac{3B}{2A} - x_1$. Pertanto, nel caso in cui il trinomio abbia una radice doppia x_0 , la curva ha un'equazione del tipo :

$$y^2 = x^2 (x + a) \quad (11.17)$$

per un opportuno $a \neq 0$. Per la **Proposizione 11.6** l'equazione complessiva delle tangenti principali in $(0,0)$ ad \mathcal{E} , è $y^2 - ax^2 = 0$, cioè le due tangenti nel punto doppio sono:

$$y - \alpha x = 0 \text{ e } y + \alpha x = 0.$$

Quindi nell'unico punto doppio di \mathcal{E} ci sono due tangenti distinte. Pertanto si possono verificare due casi: $\alpha \in \mathbb{K}$ e l'origine è un nodo, o $\alpha \notin \mathbb{K}$ e l'origine è un punto doppio isolato.

□

11.2 Legge di gruppo

L'insieme dei punti di una curva ellittica \mathcal{E} , gode di un'importante proprietà: quella di avere una struttura di gruppo abeliano rispetto all'operazione di "somma" tra punti. Vediamo cosa significa sommare punti su una curva ellittica considerando dapprima il caso di una cubica **non singolare**.

Supponiamo innanzitutto che $\text{char}\mathbb{K} \neq 2, 3$, pertanto, considerata una generica curva ellittica \mathcal{E} su \mathbb{K} , essa ha equazione $y^2 = x^3 + Ax + B$. Siano $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ due punti non necessariamente distinti di \mathcal{E} . Se consideriamo la retta P_1P_2 , per il **Teorema di Bezout**, essa interseca \mathcal{E} in esattamente tre punti. Indicato con $P'_3 = (x_{P'_3}, y_{P'_3})$ il terzo punto di intersezione tra P_1P_2 ed \mathcal{E} , denotiamo con $P_3 = (x_3, y_3)$ il suo simmetrico rispetto all'asse x e poniamo:

$$P_1 + P_2 := P_3.$$

Questa costruzione vale sia se $P_1 \neq P_2$, sia se $P_1 = P_2$. In particolare si possono presentare quattro diversi casi:

- **Caso 1:** $P_1 \neq P_2$ e $P_1, P_2 \neq \infty$.

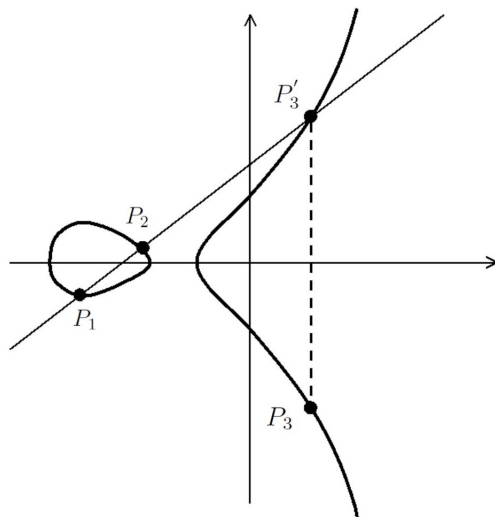


Figura 11.2: Somma tra punti di una curva ellittica nel **caso 1** con $x_1 \neq x_2$

Se $x_1 \neq x_2$, la retta P_1P_2 ha equazione:

$$y = m(x - x_1) + y_1. \quad (11.18)$$

con $m = \frac{y_2 - y_1}{x_2 - x_1}$. Per trovare le intersezioni di P_1P_2 con \mathcal{E} , sostituiamo (11.18) nell'equazione di \mathcal{E} ed otteniamo

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B \quad (11.19)$$

che può essere riscritto nella forma:

$$x^3 - m^2x^2 + (A + 2mx_1 - 2my_1)x + (B - m^2x_1^2 + 2my_1x_1 - y_1^2) = 0 \quad (11.20)$$

Le tre radici di questa cubica sono le ascisse dei tre punti di intersezione di P_1P_2 con \mathcal{E} . Poichè x_1, x_2 sono radici di (11.20) e sono elementi di \mathbb{K} e poichè il polinomio al primo membro in (11.20) è a coefficienti in \mathbb{K} , anche la terza radice $x_3 \in \mathbb{K}$. Quindi il polinomio al primo membro in (11.20) si fattorizza in

$$\begin{aligned} (x - x_1)(x - x_2)(x - x_3) &= x^3 - (x_1 + x_2 + x_3)x^2 + \\ &\quad + (x_2x_3 + x_1x_3 + x_1x_2)x - x_1x_2x_3. \end{aligned}$$

Pertanto, da (11.20) segue che $x_3 = m^2 - x_1 - x_2$ e quindi le coordinate del punto P_3 sono

$$\begin{cases} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \\ y_3 &= -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1} \right)(x_1 - x_3). \end{cases} \quad (11.21)$$

Se invece $x_1 = x_2$, la retta P_1P_2 interseca \mathcal{E} in ∞ . Pertanto, in questo caso, si ha che $P_3 = \infty$.

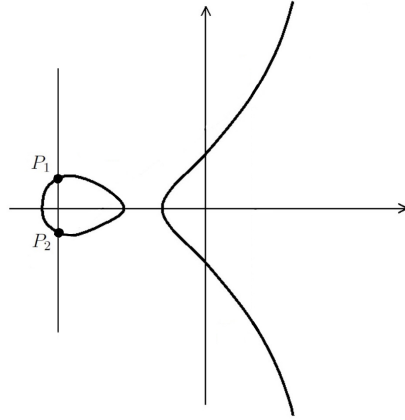


Figura 11.3: Somma tra punti di una curva ellittica nel **caso 1** con $x_1 = x_2$

- **Caso 2:** $P_1 = P_2$ e $P_1 \neq \infty$.

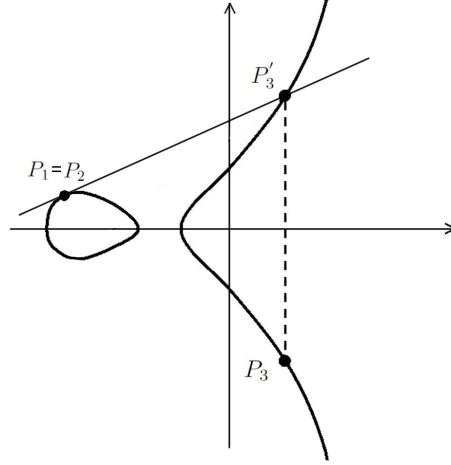


Figura 11.4: Somma tra punti di una curva ellittica nel **caso 2**

In questo caso, per la **Proposizione 11.6**, la tangente t in P_1 ad \mathcal{E} ha equazione

$$f_x(x_1, y_1)(x - x_1) + f_y(x_1, y_1)(y - y_1) = 0,$$

cioè:

$$(-3x_1^2 - A)(x - x_1) + 2y_1(y - y_1) = 0.$$

Se $y_1 \neq 0$, allora l'equazione della tangente diventa la (11.18) dove $m = \frac{3x_1^2 + A}{2y_1}$. Ora, ragionando in modo analogo al caso precedente e tenendo presente che $x_1 = x_2$, si ha che, in questo caso, le coordinate di P_3 sono:

$$\begin{cases} x_3 &= \left(\frac{3x_1^2 + A}{2y_1} \right)^2 - 2x_1 \\ y_3 &= -y_1 + \left(\frac{3x_1^2 + A}{2y_1} \right)(x_1 - x_3). \end{cases} \quad (11.22)$$

Notiamo che, se $y_1 = 0$, allora $2P_1 = \infty$.

- **Caso 3:** $P_1 \neq P_2$ e $P_1 = \infty$ (rispettivamente $P_2 = \infty$).

In questo caso, l'intersezione tra la retta $x = x_2$ (rispettivamente $x = x_1$) e la curva \mathcal{E} contiene P_1 , P_2 e $Q = (x_2, -y_2)$ (rispettivamente $Q = (x_1, -y_1)$). Pertanto si definisce $P_1 + P_2 = P_2$ (rispettivamente $P_1 + P_2 = P_1$).

- **Caso 4:** $P_1 = P_2 = \infty$.

In tal caso, per definizione, si pone $\infty + \infty = \infty$.

La costruzione sopra descritta vale anche nei casi in cui $\text{char}\mathbb{K} = 2$ e $\text{char}\mathbb{K} = 3$. Tuttavia, in tali casi, a differenza del caso precedente, le coordinate di P_3 si ricavano da quelle di P'_3 attraverso la relazione¹:

$$(x_3, y_3) = (x_{P'_3}, -a_1 x_{P'_3} - a_3 - y_{P'_3}).$$

Inoltre, sia nel caso in cui $\text{char}\mathbb{K} = 2$, che nel caso in cui $\text{char}\mathbb{K} = 3$, continuano a valere i risultati riportati nel terzo e nel quarto caso della costruzione descritta sopra. Per i primi due casi, invece, si ottengono risultati diversi in base alla caratteristica del campo, come riportato di seguito.

Se $\text{char}\mathbb{K} = 2$ e l'equazione della \mathcal{C}^3 è del tipo $y^2 + Cy = x^3 + Ax + B$, allora distinguiamo due casi:

Caso 1: $P_1 \neq P_2$ e $P_1, P_2 \neq \infty$.

- Se $x_1 \neq x_2$, le coordinate di P_3 sono:

$$\begin{cases} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 + x_1 + x_2 \\ y_3 &= C + y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_3 + x_1) \end{cases}$$

- Se $x_1 = x_2$, allora $P_3 = \infty$.

Caso 2: $P_1 = P_2$ e $P_1 \neq \infty$.

- Se $C \neq 0$, le coordinate di $P_3 = 2P_1$ sono:

$$\begin{cases} x_3 &= \frac{x_1^4 + A^2}{C^2} \\ y_3 &= C + y_1 + \left(\frac{x_1^2 + A}{C} \right) (x_3 + x_1). \end{cases}$$

- Se $C = 0$, allora $2P_1 = \infty$.

Se invece $\text{char}\mathbb{K} = 2$ e l'equazione della \mathcal{C}^3 è del tipo $y^2 + xy = x^3 + Ax^2 + B$, allora si ha:

Caso 1: $P_1 \neq P_2$ e $P_1, P_2 \neq \infty$.

- Se $x_1 \neq x_2$, le coordinate di P_3 sono:

$$\begin{cases} x_3 &= A + \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 + \frac{y_2 - y_1}{x_2 - x_1} + x_1 + x_2 \\ y_3 &= y_1 + \left(1 + \frac{y_2 - y_1}{x_2 - x_1} \right) x_3 + \frac{y_2 - y_1}{x_2 - x_1} x_1. \end{cases}$$

- Se $x_1 = x_2$, allora $P_3 = \infty$.

¹I coefficienti che compaiono nel calcolo delle coordinate di P_3 fanno ovviamente riferimento all'equazione $y^2 + y(a_1x + a_3) - x^3 - a_2x^2 - a_4x - a_6 = 0$ in coordinate non omogenee di una curva ellittica.

Caso 2: $P_1 = P_2$ e $P_1 \neq \infty$.

- Se $x_1 \neq 0$, le coordinate di $P_3 = 2P_1$ sono:

$$\begin{cases} x_3 &= \frac{x_1^4 + B}{x_1^2} \\ y_3 &= x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right)x_3 + x_3. \end{cases}$$

- Se $x_1 = 0$, allora $2P_1 = \infty$.

Se $\text{char}\mathbb{K} = 3$ e quindi l'equazione della C^3 è del tipo $y^2 = x^3 + Ax^2 + Bx + C$, allora si ha:

Caso 1: $P_1 \neq P_2$ e $P_1, P_2 \neq \infty$.

- Se $x_1 \neq x_2$, le coordinate di P_3 sono:

$$\begin{cases} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - A - x_1 - x_2 \\ y_3 &= -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3). \end{cases}$$

- Se $x_1 = x_2$, allora $P_3 = \infty$.

Caso 2: $P_1 = P_2$ e $P_1 \neq \infty$.

- Se $y_1 \neq 0$, le coordinate di $P_3 = 2P_1$ sono:

$$\begin{cases} x_3 &= \left(\frac{2Ax_1 + B}{2y_1}\right)^2 - A - 2x_1 \\ y_3 &= -y_1 + \left(\frac{2Ax_1 + B}{2y_1}\right)(x_1 - x_3). \end{cases}$$

- Se $y_1 = 0$, allora $2P_1 = \infty$.

Vale il seguente Teorema.

Teorema 11.15. *La somma dei punti su una curva ellittica \mathcal{E} soddisfa le seguenti proprietà:*

1. **Proprietà associativa:** $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ per ogni $P_1, P_2, P_3 \in \mathcal{E}$.
2. **Esistenza dell'elemento neutro:** $P + \infty = P$ per ogni $P \in \mathcal{E}$.
3. **Esistenza dell'opposto:** Dato un punto $P = (x, y)$ su \mathcal{E} , allora il punto $P' = (x, -y)$ è l'unico punto di \mathcal{E} tale che $P + P' = \infty$. Il punto P' si indica con $-P$.
4. **Proprietà commutativa:** $P_1 + P_2 = P_2 + P_1$ per ogni $P_1, P_2 \in \mathcal{E}$.

Quindi i punti di \mathcal{E} costituiscono un gruppo abeliano rispetto alla somma e l'elemento neutro di tale gruppo è ∞ .

Osservazione 11.16. Osserviamo che l'abelianità del gruppo segue banalmente dal fatto che $P_1P_2 = P_2P_1$.

Esempio 11.17. Ad esempio, la cubica a coefficienti in $GF(11)$

$$\mathcal{E} : y^2 = x^3 + x + 6$$

è una curva ellittica poiché $(4 \times 1^3 + 27 \times 6^2) \bmod 11 = 8$. Per determinare l'ordine di \mathcal{E} è sufficiente verificare se $z = x^3 + x + 6$ è un quadrato al variare di x in $GF(11)$. Per il **criterio di Eulero**, z è un quadrato in $GF(11)$ se, e solo se, $z^{\frac{11-1}{2}} \equiv 1 \bmod 11$ e quando ciò si verifica è noto che le radici quadrate modulo 11 sono $\pm z^{\frac{11+1}{4}}$.

Numero punti di \mathcal{E}

x	$(x^3 + x + 6) \bmod 11$	Quadrato	y
0	6	no	
1	8	no	
2	5	sì	4, 7
3	3	sì	5, 6
4	8	no	
5	4	sì	2, 9
6	8	no	
7	4	sì	2, 9
8	9	sì	3, 8
9	7	no	
10	4	sì	2, 9

Dalla tabella si evince che l'ordine di \mathcal{E} è 13. Quindi, $\mathcal{E} \cong Z_{13}$ e pertanto ogni punto affine di \mathcal{E} è un generatore del gruppo ad essa associato. In particolare $P = (2, 7)$ è un generatore di \mathcal{E} .

Calcoliamo $2P = P + P = (2, 7) + (2, 7)$

$$2P = \begin{cases} x_3 = \left(\frac{3x_1 + a}{2y_1} \right)^2 - x_1 - x_2 = \\ \quad = \left(((3 \times 2^2 + 1)(2 \times 7)^{-1})^2 - 2 - 7 \right) \bmod 11 = 5 \\ y_3 = \left(\frac{3x_1 + a}{2y_1} \right) (x_1 - x_3) - y_1 \\ \quad = \left(((3 \times 2^2 + 1)(2 \times 7)^{-1} \times (2 - 8)) - 2 \right) \bmod 11 = 2 \end{cases}$$

Quindi $2P = (5, 2)$.

Calcoliamo $3P = 2P + P$

$$3P = \begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 = \\ \quad = \left(((7-2)(2-5)^{-1})^2 - 5 - 2 \right) \mod 11 = 8 \\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) - y_1 = \\ \quad = ((7-2)(2-5)^{-1} \times (5-8)) - 2 \mod 11 = 3 \end{cases}$$

Pertanto, $3P = (8, 3)$.

Procedendo in questo modo, si ottiene

$$\begin{array}{lll} P = (2, 7) & 2P = (5, 2) & 3P = (8, 3) \\ 4P = (10, 2) & 5P = (3, 6) & 6P = (7, 9) \\ 7P = (7, 2) & 8P = (3, 5) & 9P = (10, 9) \\ 10P = (8, 8) & 11P = (5, 9) & 12P = (2, 4) \end{array}$$

e chiaramente $13P = \infty$.

□

Se \mathbb{K} è finito, la struttura generale del gruppo associato ad una curva ellittica è ben nota, come mostra il seguente teorema.

Teorema 11.18. *Sia \mathcal{E} una curva ellittica sul campo finito $GF(q)$. Allora*

$$\mathcal{E} \cong Z_n \quad \text{oppure} \quad \mathcal{E} \cong Z_{n_1} \oplus Z_{n_2}$$

dove n, n_1, n_2 sono opportuni interi ≥ 1 e $n_1 \mid n_2$.

11.3 Numero di punti di una curva ellittica

In diverse applicazioni in crittografia vengono utilizzate le curve ellittiche. Tali curve, se sono a coefficienti in un campo finito, hanno un numero finito di punti. Tale numero si indica con N ed è detto **ordine della curva \mathcal{E}** .

Un'altra grandezza importante nell'ambito della crittografia su curve ellittiche, è l'**ordine di un punto** della curva. Data una curva ellittica \mathcal{E} ed un punto $P \in \mathcal{E}$, si dice ordine di P il più piccolo intero positivo k , se esiste, tale che $kP = \infty$. Se tale intero non esiste, si dice che P ha ordine infinito.

Vediamo ora di dare una stima del numero dei punti di una curva ellittica \mathcal{E} definita su $GF(q)$ con $q = p^r$, p primo. Supponiamo che \mathcal{E} abbia equazione

$$y^2 = x^3 + ax + b. \quad (11.23)$$

Abbiamo visto che se $p = 2$, \mathcal{E} è data dalle equazioni

$$y^2 + cy = x^3 + ax + b \quad \text{o} \quad y^2 + xy = x^3 + ax + b \quad (11.24)$$

mentre se $p = 3$, \mathcal{E} è definita da

$$y^2 = x^3 + ax^2 + bx + c. \quad (11.25)$$

E' facile vedere che una curva ellittica ha al più $2q + 1$ punti di $GF(q)$, cioè ∞ insieme con $2q$ coppie (x, y) con x, y elementi di $GF(q)$ che soddisfano (11.23) (o (11.24) o (11.25) se $p = 2$ o 3 , rispettivamente). Infatti, per ciascuno dei q possibili valori di x ci sono al più 2 valori di y che soddisfano (11.23).

Poiché solo la metà degli elementi di $GF(q)^*$ hanno radici quadrate ci si aspetta che il numero N dei punti di una curva ellittica sia circa il numero dei punti di $GF(q)$. Più precisamente, sia χ il carattere quadratico di $GF(q)$. Cioè χ è la funzione che a $x \in GF(q)^*$ associa ± 1 a seconda che x abbia o meno una radice quadrata in $GF(q)$ (e prendiamo $\chi(0) = 0$). Per esempio, se $q = p$ è un primo, allora $\chi(x) = \left(\frac{x}{p}\right)$ è il simbolo di Legendre. Pertanto, in tutti i casi, il numero delle soluzioni $y \in GF(q)$ dell'equazione $y^2 = u$ è uguale a $1 + \chi(u)$ e quindi il numero delle soluzioni di (11.23) (contando anche il punto ∞) è

$$1 + \sum_{x \in GF(q)} (1 + \chi(x^3 + ax + b)) = q + 1 + \sum_{x \in GF(q)} \chi(x^3 + ax + b). \quad (11.26)$$

Ci si aspetta che $\chi(x^3 + ax + b)$ possa assumere con la stessa frequenza i valori $+1$ e -1 . Il seguente Teorema fornisce dei limiti più precisi per il numero dei punti di \mathcal{E} :

Teorema 11.19. (Teorema di Hasse)

Sia \mathcal{E} una curva ellittica sul campo finito $GF(q)$. Allora l'ordine N di \mathcal{E} soddisfa

$$|N - (q + 1)| \leq 2\sqrt{q}. \quad (11.27)$$

Osservazione 11.20. Osserviamo che (11.27) equivale a

$$(\sqrt{q} - 1)^2 \leq N \leq (\sqrt{q} + 1)^2 \quad (11.28)$$

Esempio 11.21. Si consideri la curva ellittica $\mathcal{E} : y^2 = x^3 + x + 6$ a coefficienti in $GF(11)$, vale che

$$5, 36 \sim (\sqrt{11} - 1)^2 \leq N = 13 \leq (\sqrt{11} + 1)^2 \sim 18, 63.$$

□